



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/425,736	10/22/1999	YUSAKU FUJII	991176	9951

38834 7590 12/02/2005

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP
1250 CONNECTICUT AVENUE, NW
SUITE 700
WASHINGTON, DC 20036

EXAMINER

KHOSHNOODI, NADIA

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 12/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/425,736	Applicant(s) FUJII ET AL.	
	Examiner Nadia Khoshnoodi	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 06 September 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3-12 and 14-22 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1, 3-12, & 14-22 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 22 October 1999 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendments

Claims 1, 3-12, and 14-22 are pending in this application. Applicant's amendments/arguments filed on 9/6/2005 have been fully considered and therefore the claims are rejected under new grounds. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Drawings

The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the "illegal access discriminating apparatus" must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will

Art Unit: 2137

be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

Claim 1 is objected to because of the following informalities: "informational" in line 3 of the claim may be misspelled, where the intended spelling may have been "information."

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 11 and 22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claims 11 and 22:

These claims recite the limitation "the service providing system" in line 3. Due to the amendments made to claims 1 and 12, a service providing system is no longer previously introduced in the parent claim. Therefore, there is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

II. Claims 1, 5, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Moussa et al., United States Patent No. 6,035,406 and further in view of McNair, United States Patent No. 5,276,444

As per claims 1 and 12:

Moussa et al. substantially teach an illegal access discriminating apparatus comprising: a first storing unit for temporarily storing the latest pair of ID information and organic information inputted by a user when the user is being authentication; a second storing unit for storing pairs of ID information and organic information which were inputted by arbitrary users within predetermined time wherein said ID information and organic information is transferred from said first storing unit to said second storing unit after each authentication (col. 3, lines 24-33); and a comparing and collating unit for comparing and collating the latest inputted ID information and organic information with all of ID information and organic information stored in second storing unit which were inputted and not previously registered in the past (col. 3, lines 24-33 and col. 4, lines 56-64).

Not explicitly disclosed is a control unit for discriminating authentication demand by an attacker by counting the number of said comparing-collating results which satisfy predetermined conditions and judging authentication demand as the one by an attacker if said counted number

Art Unit: 2137

exceeds predetermined value. However, McNair teaches a threshold per biometric sample type that can possibly be used by each individual in order to indicate an attacker in the event of numerous unsuccessful authentication attempts. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Moussa et al. to determine that the numerous unsuccessful authentication attempts are a result of an attacker trying to gain access. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since McNair suggests the feature of only allowing those requesters that reach a certain level of authentication using one type of biometric sample to supply another type of sample up to a certain threshold until all possibilities are exhausted and the requester is either authenticated or locked out from being authenticated (col. 13, lines 38-68).

As per claim 5:

Moussa et al. and McNair substantially teach the system/method as applied to claim 1 above. Furthermore, Moussa et al. teaches a person trying to gain access enters a password, then transmits the biometric-password for identification along with the hardware code and identifies the payer using the biometric sample (fig. 2).

III. Claims 3-4, 6-11, and 14-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moussa et al., United States Patent No. 6,035,406 and McNair, United States Patent No. 5,276,444 as applied to claims 1 and 12 above, and further in view of Gressel, United States Patent No. 6,311,272.

As per claim 3:

Moussa et al. and McNair substantially teach the system/method as applied to claim 1 above. Moussa et al. and McNair fail to teach control unit determines that there is the authentication demand by the illegal access person in the case where the ID information does not coincide and the organic information coincides or the case where the ID information coincides and the organic information does not coincide on the basis of the output of the comparing and collating unit. Gressel teaches two typical proximity thresholds for biometric sampling, which are monitored for imposters attempting to enter unauthorized (col. 10, lines 26-34). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because it would allow unauthorized entries to be halted.

As per claim 4:

Moussa et al. and McNair substantially teach the system/method as applied to claim 1 above. Moussa et al. and McNair fail to teach a timer unit for measuring a time and wherein the ID information and organic information, which were inputted in the past after the elapse of a predetermined time from the storage on the basis of time information measured by the timer unit are erased and excluded from targets of the comparison and collation. Gressel teaches upon successful completion of the biotest, the user's biometric features are encoded into the smart card. The original template threshold value is a parameter, which is typically determined by the system application owner, depending on the application. (col. 12, lines 42-48). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair, because it would allow only a reasonable amount of time to transfer the biometric features, thus discouraging break-ins. The thresholds and templates are only read from the user.

As per claim 6:

Moussa et al. and McNair substantially teach the system/method as applied to claim 1 above. Moussa et al. and McNair fail to teach the inputted organic information and the organic information which was inputted in the past coincide, the control unit detects a combination in which the organic information coincides and the ID information differs, and when the number, the control unit determines that there is the authentication demand by the illegal access person. Gressel teaches a false rejection rate rejects a percentage of individuals when the meeting of the two (false acceptance rate and false rejection rate) nears the threshold (col. 10, lines 5-23). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because it would allow the attempted user to be authenticated.

As per claim 7:

Moussa et al. and McNair substantially teach the system/method as applied to claim 1 above. Moussa et al. and McNair fail to teach an ID information comparing unit for comparing the inputted ID information and the ID information which was inputted in the past and generating a signal indicative of coincidence or dissidence and an organic information collating unit for comparing the inputted organic information and the organic information which was inputted in the past, generating a signal indicative of coincidence of the organic information in the case where a value of a predetermined coincidence degree or more is obtained and generating a signal indicative of dissidence of the organic information in the case where a value less than the predetermined coincidence degree is obtained. Gressel teaches a percentage of the population would be rejected and the guards would be signaled (col. 10, lines 48-54). Also, Gressel teaches a false acceptance rate and false rejection rate (col. 9, lines 50-67) and upon comparison with the threshold value, a large subgroup would be allowed entry (col. 9, lines 50-67 and col. 10, lines 1-

5). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because it would allow personal information to be used in records for authorization with a specific individual.

As per claim 8:

Moussa et al. and McNair substantially teach the system/method as applied to claim 1 above. Moussa et al. and McNair fail to teach a timer unit for measuring a time and wherein the ID information and organic information, which were inputted in the past after the elapse of a predetermined time from the storage on the basis of time information measured by the timer unit are erased and excluded from targets of the comparison and collation. Gressel teaches upon successful completion of the biotest, the user's biometric features are encoded into the smart card, the original template threshold value is a parameter, which is typically determined by the system application owner, depending on the application. (col. 12, lines 42-48). 11: would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because it would allow only a reasonable amount of time to transfer the biometric features, thus discouraging break-ins. The thresholds and templates are only read from the user.

As per claim 9:

Moussa et al. and McNair substantially teach the system/method as applied to claim 1 above. Moussa et al. and McNair fail to teach the storing unit stores a telephone number serving as a transmitting source and a terminal position such as a network address or the like together with the ID information and organic information which were inputted in the past. Gressel teaches secret keys and random numbers are internally generated in smart cards and security application modules in terminal devices. Biometric data in a secure system is equivalent to pins and

passwords. (col. 11, lines 47-57). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair to designate a personal ID as telephone numbers and biometric data to increase the security of the apparatus.

As per claim 10:

Moussa et al. and McNair substantially teach the system/method as applied to claim 1 above. Moussa et al. and McNair fail to teach an authentication demand terminal address recording unit for recording the number of times of authentication demand every terminal address and the same terminal access detecting unit for detecting that the authentication demand of a predetermined number or more has been performed within a predetermined time with reference to the authentication demand terminal address, activating the comparing and collating unit and the control unit and allowing an illegal access to be discriminated. Gressel teaches the use of an original template threshold value, which sets values that are larger than the user's smart card threshold value. This threshold value is incremented appropriately and thus records the demands on the authentication process Gressel teaches the use of a biotest to compare fingerprints where only 3 percent of the population would be rejected (col. 12, lines 45-51). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because preliminary screening of users reduces fraudulent access to the authentication system, thus reducing processor time.

As per claim 11:

Moussa et al. and McNair substantially teach the system/method as applied to claim 1 above. Moussa et al. and McNair fail to teach that when it is determined that there is the authentication demand by the illegal access person, the control unit automatically notifies an

Art Unit: 2137

administrator of the service providing system of a result of the discrimination. Gressel teaches a rejection results in the further processing of the applicant by a guard (col. 10, lines 48-54). The guard is comparable to an administrator. It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because the use of an administrator's intervention would facilitate the accuracy of the authentication process.

As per claim 14:

Moussa et al. and McNair substantially teach the system/method as applied to claim 12 above. Moussa et al. and McNair fail to teach a control step, it is determined that there is the authentication demand by the illegal access person in the case where the ID information does not coincide and the organic information does not coincide on the basis of the output in the comparing and collating step. Gressel teaches that 3% of the population would be rejected regardless of the value of the threshold. Human intervention then becomes necessary to process the applicant. (col. 10, lines 48-54) It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because of the need to resolve the authentication of applicants who qualify for access with a valid threshold value, but not qualifying organic information.

As per claim 15:

Moussa et al. and McNair substantially teach the system/method as applied to claim 12 above. Moussa et al. and McNair fail to teach telephone number serving as a transmitting source, a terminal position such as a network address, and an input time in correspondence to the ID information and organic information which were inputted in the past are stored and in the control step, it is determined that there is the authentication demand by the illegal access person in the case where the comparison result in the comparing and collating step between the inputted

Art Unit: 2137

from a same terminal position within a predetermined time indicates dissidence. Gressel teaches secret keys and random numbers are internally generated in smart cards and security application modules in terminal devices. Biometric data in a secure system is equivalent to pins and passwords. (col. 11, lines 47-62). An original template resides in the terminal while a threshold value is in a user's smart card (col. 12, lines 46-51). 3% of the population would be rejected regardless of the value of the threshold. Human intervention then becomes necessary to process the applicant. (col. 10, lines 48-54) It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair to designate a personal ID as telephone numbers and biometric data to increase the security of the apparatus, to store the information to use for authentication, and because of the need to resolve the authentication of applicants who qualify for access with a valid threshold value, but not qualifying organic information.

As per claim 16:

Moussa et al. and McNair substantially teach the system/method as applied to claim 12 above. Moussa et al. and McNair fail to teach past ID information has a serial number for the inputted ID information or not is discriminated and, when it is determined that the past ID information has the serial number, it is determined that there is the authentication demand by the illegal access person at a predetermined designated number of times. Gressel teaches a fingerprint scan is used in a biotest scan, the threshold value has little effect on the test, and an illegal access person has a limited number of tries because of their fear of being caught (col. 10, lines 40-47). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because a biotest scan would deter unauthorized access attempts and minimize the authentication systems use of the processor.

Art Unit: 2137

As per claim 17:

Moussa et al. and McNair substantially teach the system/method as applied to claim 12 above. Moussa et al. and McNair fail to teach the inputted organic information and the organic information, which was inputted in the past coincide, a combination in which the organic information coincides and the ID information differs is detected, and when the number of the combinations reaches a predetermined number, it is determined that there is the authentication demand by the illegal access person. Gressel teaches two typical proximity thresholds for biometric sampling, which are monitored for imposters attempting to enter unauthorized (col. 10, lines 26-47). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because it would allow unauthorized entries to be halted.

As per claim 18:

Moussa et al. and McNair substantially teach the system/method as applied to claim 12 above. Moussa et al. and McNair fail to teach an ID information comparing unit for comparing the inputted ID information and the ID information which was inputted in the past and generating a signal indicative of coincidence or dissidence and an organic information collating unit for comparing the inputted organic information and the organic information which was inputted in the past, generating a signal indicative of coincidence of the organic information in the case where a value of a predetermined coincidence degree or more is obtained and generating a signal indicative of dissidence of the organic information in the case where a value less than the predetermined coincidence degree is obtained. Gressel teaches a percentage of the population would be rejected and the guards would be signaled (col. 10, lines 48-54). Also, Gressel teaches a false acceptance rate and false rejection rate (col. 9, lines 50-67) and upon comparison with the

Art Unit: 2137

threshold value, a large subgroup would be allowed entry (col. 9, lines 50-67 and col. 10, lines 1-5). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because it would allow personal information to be used in records for authorization with a specific individual.

As per claim 19:

Moussa et al. and McNair substantially teach the system/method as applied to claim 12 above. Moussa et al. and McNair fail to teach a timer unit for measuring a time and wherein the ID information and organic information, which were inputted in the past after the elapse of a predetermined time from the storage on the basis of time information measured by the timer unit are erased and excluded from targets of the comparison and collation. Gressel teaches upon successful completion of the biotest, the user's biometric features are encoded into the smart card. The original template threshold value is a parameter, which is typically determined by the system application owner, depending on the application. (col. 12, lines 42-48). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because it would allow only a reasonable amount of time to transfer the biometric features, thus discouraging break-ins. The thresholds and templates are only read from the user.

As per claim 20:

Moussa et al. and McNair substantially teach the system/method as applied to claim 12 above. Moussa et al. and McNair fail to teach a timer unit for measuring a time and wherein the ID information and organic information, which were inputted in the past after the elapse of a predetermined time from the storage on the basis of time information measured by the timer unit are erased and excluded from targets of the comparison and collation. Gressel teaches upon

Art Unit: 2137

successful completion of the biotest, the user's biometric features are encoded into the smart card. The original template threshold value is a parameter, which is typically determined by the system application owner, depending on the application. (col. 12, lines 42-48) The ID module detects a payee or payer by conducting a re-registration check (col., 9, lines 33-41). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because it would allow only a reasonable amount of time to transfer the biometric features, thus discouraging break-ins. The thresholds and templates are only read from the user.

As per claim 21:

Moussa et al. and McNair substantially teach the system/method as applied to claim 12 above. Moussa et al. and McNair fail to teach an authentication demand terminal address recording unit for recording the number of times of authentication demand every terminal address and the same terminal access detecting unit for detecting that the authentication demand of a predetermined number or more has been performed within a predetermined time with reference to the authentication demand terminal address, activating the comparing and collating unit and the control unit and allowing an illegal access to be discriminated. Gressel teaches the use of an original template threshold value, which sets values that are larger than the user's smart card threshold value. This threshold value is incremented appropriately and thus records the demands on the authentication process. Gressel teaches the use of a biotest to compare fingerprints where only 3 percent of the population would be rejected (col. 12, lines 45-51). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because preliminary screening of users reduces fraudulent access to the authentication system, thus reducing processor time.

Art Unit: 2137

As per claim 22:

Moussa et al. and McNair substantially teach the system/method as applied to claim 12 above. Moussa et al. and McNair fail to teach that when it is determined that there is the authentication demand by the illegal access person, the control unit automatically notifies an administrator of the service providing system of a result of the discrimination. Gressel teaches a rejection results in the further processing of the applicant by a guard (col. 10, lines 48-54). The guard is comparable to an administrator. It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because the use of an administrator's intervention would facilitate the accuracy of the authentication process.

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 5,715,518
2. US Patent No. 5,892,838
3. US Patent No. 5,229,764

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.



Nadia Khoshnoodi
Examiner
Art Unit 2137
11/25/2005

NK



MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137